MASTER OF SCIENCE
IN
SYSTEMS TECHNOLOGY

TERRAIN CATEGORIZATION USING MULTITEMPORAL INFRARED IMAGERY

Julie M. Alfieri-Lieutenant, United States Navy
B.S., United States Naval Academy, 1996
Masters of Science in Systems Technology-June 2001
Advisor: Richard C. Olsen, Department of Physics
Second Reader: Alan A. Ross, Navy Tactical Exploitation of National Capabilities (TENCAP) Chair Professor

Terrain Categorization (TERCAT) in remote sensing is used extensively by the United States Military to conduct Intelligence Preparation of the Battlefield (IPB). This thesis explores the feasibility of exploiting multitemporal infrared imagery for the purpose of TERCAT. Two littoral locations were imaged multiple times from August through October 1998 using National Technical Means (NTM). Images were merged and analyzed using commercial off the shelf (COTS) technology, producing TERCAT maps of both target areas. Both supervised and unsupervised classification methods were used in this process. The TERCAT maps were compared with ground truth measurements to determine the overall classification accuracy. Accuracy levels above eighty percent were achieved. This variation on traditional change detection methods provides an alternative single-sensor approach to terrain categorization that can be utilized by the military.

DoD KEY TECHNOLOGY AREA: Sensors

KEYWORDS: Remote Sensing, Sensor Fusion, TERCAT

VULNERABILITY ASSESSMENT THROUGH PREDICTIVE MODELING OF IEEE 802.11 STANDARD WIRELESS LOCAL AREA NETWORKS

Shane P. Halloran-Lieutenant, United States Navy
B.S., United States Naval Academy, 1995
Master of Science in Systems Technology-June 2001
Advisors: Tri T. Ha, Department of Electrical and Computer Engineering
CAPT James R. Powell, USN, Information Warfare Academic Group

The development of the IEEE 802.11 standard for wireless local area networks (WLANs) has greatly accelerated the commercial development of wireless technology for enterprise network solutions. Government and military organizations are also benefiting from the competition and interoperability fostered under the international standard. Given the decreasing cost, and proliferation of wireless networking technology, organizations are foregoing the expansion of cumbersome ethernet networks, and turning to cheap, available wireless architectures to augment data communication and processing needs.

Wireless technology availability coupled with the U.S. military's trend of looking to commercial-off-the-shelf (COTS) communication and computing solutions necessitate an awareness of the characteristics of WLANs. The argument for research is bolstered when considering how the ease of implementation and low system maintenance costs make it probable that second or third world entities at odds with US interests may use COTS wireless technology. Should the U.S. confront adversaries that have integrated command and control circuits consisting of WLANs, or come under attack from groups that know how to exploit our own, it will be necessary to have analyzed WLAN characteristics.

This thesis intends to research the current industry technology and standards driving WLAN interoperability, and determine which vendor's components are likely to be seen in world markets. Finally, the thesis will analyze a WLAN communications link at NPS to determine feasibility of emissions/intercept field mapping using a modular software and hardware suite.

DoD KEY TECHNOLOGY AREAS: Command, Control and Communications, Computing and Software, Electronics, Electronic Warfare, Sensors, Other (Wireless LANs)

KEYWORDS: Wireless Local Area Networks, IEEE 802.11, Exploitation, Vulnerability, Link Analysis, Radio Propagation, Network Security, Information Operations

INFLUENCE NET MODELING: THE NARCOTICS NETWORK IN COLOMBIA

Joshua C. Himes-Lieutenant, United States Navy
B.A., University of Pennsylvania-1993
Master of Science in Systems Technology-June 2001
and
Mark W. Garrett-Major-United States Army
B.L.A., Texas Tech University-1988
Master of Science in Information Systems and Operations-March 2001
Advisors: LT Raymond R. Buettner, USN, Information Warfare Academic Group
Jeanne K. Giraldo, Department of National Security Affairs

The purpose of this thesis is to conduct the research necessary to develop a situational influence assessment model to identify critical indicators that will assist the USSOUTHCOM in identifying potential key centers of gravity in the fight against illicit drug production and narcotrafficking in Colombia. Efforts to combat the narcotics network directly support the USSOUTHCOM mission and are integral to U.S. National Security. Unlike the traditional military threats of the Cold War and previous decades, to include *Operation Desert Storm*, this problem set is far more complex and complicated with roots and foundations that date back to the development of Colombia as a nation-state. It is the strategic dilemma that is posed by this asymmetric threat that reflects the type of problems that will be encountered by the military of the 21st century. Unlike the traditional land/sea/air combined warfare that the U.S. dominates globally, the threats of the 21st century will look much like Colombia – small, packetized, networked organizations with the ability to operate and inflict casualties below the threshold of our traditional military mechanisms. Improved decision support systems to model this type of problem are needed. This thesis suggests a number of modifications to an existing model, SIAM, in order to enhance its usefulness both for decision makers and intelligence collectors.

DoD KEY TECHNOLOGY AREAS: Other (Information Operations, Intelligence Information Management)

KEYWORDS: Information Operations, Intelligence, Decision Support Systems, Influence Net Modeling, Colombia

COMPUTER NETWORK DEFENSE: A SURVEY OF NETWORK TRACING TECHNIQUES

John R. Hollander-Major, United States Marine Corps
B.S., Marquette University, 1989
Master of Science in Systems Technology-June 2001
Advisors: CAPT James Powell, USN, Information Warfare Academic Group
John McEachen, Department of Electrical and Computer Engineering

With the growth of the Internet, the World Wide Web, and digital networks throughout the Department of Defense (DoD), the amount of information and resources available nearly instantaneously greatly impacts operations within DoD and each service. Because of this impact, the reliability, integrity and availability of data has become critical to the success of the Department's mission. As part of the security posture of DoD, a layered defense is integrated into its digital networks, which is implemented as a passive measure to meet DoD's security needs. These defenses, however, are able to identify the origin of attacks only after traditional investigative techniques are employed. This thesis looks at al of the research being conducted in academia, in the commercial sector, and within the government to address the traceback problem, the means to identify an attacker's Internet source location via automated methods.

DoD KEY TECHNOLOGY AREAS: Command, Control and Communications, Computing and Software, Sensors, Other (Computer Security, Information Operations)

KEYWORDS: Traceback, CNA, CNE, CND, Network Security, DNO, IO

3D VISUALIZATION OF TACTICAL COMMUNICATIONS FOR PLANNING AND OPERATIONS USING VIRTUAL REALITY MODELING LANGUAGE (VRML) AND EXTENSIBLE 3D (X3D)

Michael G. Hunsberger-United States Air Force
B.S., Rochester Institute of Technology, 1996
Master of Science in Systems Technology-June 2001
Master of Science in Computer Science-June 2001
Advisors: Don Brutzman, Undersea Warfare Academic Group
MAJ David Laflam, USA, U.S. Army Modeling and Simulation Office
Dan Boger, Command, Control, Communications, Computers, and Intelligence Academic Group

The military is increasingly reliant on communication networks for day-to-day tasks as well as large-scale military operations. Tactical communications networks are growing progressively more complex as the amount of information required on the battlefield increases. Communication planners require more advanced tools to perform and manage signal-planning activities. This work examines the use of 3D visualizations to assist in tactical signal planning. These visualizations are developed using Virtual Reality Modeling Language (VRML), Extensible 3D (X3D) graphics, and Distributed Information Simulation (DIS) for network connectivity.

These visualizations and the connectivity provide signal planners the ability to generate 3D scenarios quickly identifying problems such as frequency interference, connectivity problems, and marginal-coverage areas. Network connectivity also provides a collaborative planning environment for geographically dispersed units.

The NATO Global Hub Land C2 Information Exchange Data Model (LC2IEDM) is a semantic model designed for information passing between systems. This work also examines LC2IEDM for its ability to represent tactical communication plans and facilitate the autogeneration of 3D scenarios.

DoD KEY TECHNOLOGY AREAS: Command, Control, Communications, Modeling and Simulation

KEYWORDS: 3D Visualizations, Virtual Reality Modeling Language (VRML), Extensible 3D (X3D), Tactical Communications, Communications Planning, NATO Global Hub, Land C2 Information Exchange Data Model (LC2IEDM)

EXPERIMENTATION METHODOLOGY FOR EVALUATING OPERATIONAL INFOCON IMPLEMENTATIONS

Richard A. Kimmel-DoD Civilian
B.S., Chapman University, 1988
Masters of Science in Systems Technology-June 2001
Advisors: W.G. Kemple, Command, Control, Communications, Computers, and Intelligence Academic Group
S.P. Gallup, Institute for Joint Warfare Analysis

Information Operation Condition (INFOCON) implementations and specifically the impact these implementations can have on warfighting command and control processes are not yet widely understood or appreciated by the majority of the operating forces. INFOCON actions are designed to heighten or reduce defensive posture uniformly, to defend against computer network attacks, and to mitigate sustained damage to the DoD infrastructure. Experimentation is required to explore the effects on certain command and control processes under various INFOCON conditions. This thesis explored requirements for conducting these INFOCON experiments and resulted in the development of an INFOCON experimental design methodology that can be used as a framework for designing and conducting INFOCON experiments in the field. INFOCON experimentation will provide insights and a better understanding of the effects that these implementations will have on the ability of a commander to command and control his or her forces.

DoD KEY TECHNOLOGY AREA: Command, Control and Communications

KEYWORDS: Information Operation Condition (INFOCON), Experimentation, Network Centric Warfare

VULNERABILITIES ASSOCIATED WITH REMOTE ACCESS TO TIMESTEP VIRTUAL PRIVATE NETWORKS (VPNs)

Joseph A. Matos-Major, United States Marine Corps
B.A., Virginia Tech, 1989
Master of Science in Systems Technology-June 2001
Advisor: Dan Warren, Department of Computer Science
Second Reader: John Osmundson, Command, Control, Communications, Computers, and Intelligence Academic Group

As Marine Corps requirements for Internet access continue to increase, so do the concerns about network security. One of the key components in the Marine Corps network security architecture is the employment of TimeStep Virtual Private Network (VPN) products to protect the Marine Corps Enterprise Network (MCEN). These VPN products provide security through authentication, confidentiality, and data integrity. Remote access to the MCEN via TimeStep VPNs provides the flexibility, security, and global connectivity required in today's high operations tempo.

Despite the benefits TimeStep VPNs provide to deployed users, the risks associated with remote access remain unclear. In this thesis, the author begins by identifying and evaluating vulnerabilities associated with remote user access to TimeStep VPNs via dial up modems, cable TV modems, and Digital Subscriber Lines (DSL). After the vulnerabilities have been identified, the author proposes policies and procedures that can mitigate these vulnerabilities. The aim of this study is to provide systems administrators and remote users of the MCEN useful insights into the threats that exist when using TimeStep VPNs and assistance in lessening their impact.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Virtual Private Networks, Computer Network Attack, Computer Security, Computing and Software, Network Security

INFORMATION SECURITY REQUIREMENTS FOR A COALITION WIDE AREA NETWORK

Susan C. McGovern-Lieutenant, United States Navy
B.A., University of California Los Angeles, 1992
Master of Science in Systems Technology-June 2001
Advisor: Cynthia E. Irvine, Department of Computer Science
Second Reader: Orin E. Marvel, Command, Control, Communications, Computers, and Intelligence Academic Group

To achieve information superiority in a coalition environment the U.S. has to seamlessly integrate coalition members, both NATO and Non-NATO, into its command and control processes along all echelons of military operations. In a coalition environment, it is extremely challenging to fuse multinational information systems to achieve seamless integration. This thesis focuses on the security issues that are involved in establishing coalition network interoperability. The coalition environment is defined in terms of purpose, command structure, mission area, and control functions. Network and information protection are discussed in terms of minimizing the threats to information systems security. Coalition information system user requirements are defined and some of the security mechanisms required to meet those requirements are discussed. Current solutions to secure coalition network interoperability are surveyed, followed by conclusions, recommendations and areas for further study.

DoD KEY TECHNOLOGY AREAS: Battlespace Environment, Command, Control, and Communications, Other (Information Assurance)

KEYWORDS: Battlespace Environment, Command, Control, and Communications (3), Information Assurance

EXPLOITATION OF AN IEEE 802.11 STANDARD WIRELESS LOCAL AREA NETWORK THROUGH THE MEDIUM ACCESS CONTROL (MAC) LAYER

William S. Myers-Lieutenant, United States Navy
B.S., United States Naval Academy, 1994
Master of Science in Systems Technology-June 2001
Advisors: Tri T. Ha, Department of Electrical and Computer Engineering
R. Clark Robertson, Department of Electrical and Computer Engineering

Wireless Local Area Networks (WLAN) have increased in popularity and use in recent years and with this has come a respective increase in interest in ways to exploit these networks. Among the varying proprietary and standardized implementations available, the IEEE 802.11 standard WLAN has become the predominant implementation of WLAN in use today. This thesis examines the Medium Access Control (MAC) layer of the IEEE 802.11 WLAN for security weaknesses and vulnerabilities that can be exploited to eavesdrop, modify or inject data, or gain access to a WLAN. The functionality of the MAC layer in the IEEE 802.11 standard is reviewed and specific known attacks against it are presented and analyzed. Finally, a review of a current proposal to enhance the security of the IEEE 802.11 standard is presented.

DoD KEY TECHNOLOGY AREAS: Command, Control and Communications, Computing and Software, Information Operations

KEYWORDS: Wireless Local Area Networks, IEEE 802.11, Exploitation, Medium Access Control Layer, Cryptology, Network Security, Information Operations

TERRAIN CATGORIZATION USING MULTITEMPORAL SYNTHETIC APERATURE RADAR (SAR)

James G. Reese, Jr.-Lieutenant, United States Navy
B.S., Pennsylvania State University, 1995
Master of Science in Systems Technology-June 2001
Advisors: Richard C. Olsen, Department of Physics
Alan A. Ross, Navy Tactical Exploitation of National Capabilities (TENCAP) Chair Professor

Multitemporal synthetic aperture radar (SAR) imagery is exploited for the purpose of Terrain Categorization (TERCAT). This thesis explores using SAR data from National Technical Means (NTM) to construct detailed TERCAT maps. Two littoral military locations were imaged multiple times over a three-month period. These images were registered to each other and combined to form multi-band composite images. Unsupervised and supervised classification techniques were then used to construct TERCAT maps of the two littoral military locations. The unsupervised and supervised classification techniques used unique spectral elements in the multi-band composite images to assign each pixel in the composite images to a terrain class. The TERCAT maps were compared with ground truth measurements to determine the overall categorization accuracy with good results. The military utility of the TERCAT techniques and products was explored with an emphasis on the intelligence value.

DoD KEY TECHNOLOGY AREA: Sensors

KEYWORDS: Remote Sensing, Sensor Fusion, TERCAT

USING MULTIPLE COLLABORATIVE AGENTS FOR ADAPTIVE QUALITY OF SERVICE MANAGEMENT OF C4ISR NETWORKS

Raymond A. Rivera-Lieutenant, United States Navy
B.S., United States Naval Academy, 1994
Master of Science in Systems Technology-June 2001
Master of Science in Information Technology Management-June 2001
Advisors: Alex B. Bordetsky, Information Systems Academic Group
John S. Osmundson, Command, Control, Communications, Computers, and Intelligence Academic Group

This research explores the potential of agent technology for adaptive quality of service (QOS) management of c4isr networks. With the growing emphasis on information superiority, any time savings or additional utilization of resources enabled by effective network management becomes increasingly important. Intelligent agents are ideal for assessing information, adapting to dynamic conditions, and predicting future network conditions. In the kernel of the proposed multiple agent system (MAS) testbed are agent shared memory and majority rule architectures for agent conflict resolution. The case based reasoning (CBR) technique provides the foundation for building the agents' shared memory of qos management solutions and allows the individual agents to share their associations of feedback controls in response to application and user qos profiles. Based on the telecommunications management network (TMN) functionality, we use this agent architecture to effectively translate the warfighter's service layer application requirements across the network. The fundamental frameworks of service level management (SLM) and policy based management (PBM) serve as cornerstones in effectively gathering and applying specific application requirements. Finally, we utilize these techniques to investigate an actual C4I application at the pacific region network operating center (PRNOC) in Wahiawa, Hawaii as the real-world focal point of the thesis.

DoD KEY TECHNOLOGY AREA: Command, Control, and Communications

KEYWORDS: Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), Agent Technology, Quality of Service (QoS), Case Based Reasoning (CBR), Service Level Management (SLM), Policy Based Management (PBM), Telecommunications Management Network (TMN)

VULNERABILITY ASSESSMENT OF WIRELESS DATA NETWORK SIGNAL TRANSMISSIONS

Keith E. Shaffer-Captain, United States Marine Corps
B.S., Old Dominion University, August 1992
Master of Science in Systems Technology-June 2001
Advisor: Tri T. Ha, Department of Electrical and Computer Engineering
Second Reader: Dan C. Boger, Command, Control, Communications, Computers, and Intelligence Academic Group

The abstract is for official use only.

DoD KEY TECHNOLOGY AREA: Command, Control, and Communications

KEYWORDS: Wireless LAN, Wireless Bridge, IEEE 802.11, IEEE 802.16

WORLDWIDE METEOROLOGICAL AND OCEANOGRAPHIC DATA DISTRIBUTION USING THE GLOBAL BROADCAST SERVICE

William L. Wheeler Jr.-Captain, United States Marine Corps
B.B.A., University of Tennessee, 1992
Master of Science in Systems Technology-June 2001
Advisor: LCDR Steve J. Iatrou, USN, Information Warfare Academic Group
Second Reader: Charles M. Racoosin, Naval Space Systems Academic Chair

The Fleet Numerical Meteorology and Oceanography Center (FNMOC) produces large meteorological and oceanographic (METOC) data files in support of regional METOC centers worldwide. These data files can be from 50 megabytes to 1 gigabyte in size and can take up to one hour and twenty-eight minutes to send across a T-1 (1.544 Megabits per second (Mbps)) line due to physical limitations and network delays. However, not all of FNMOC's customers have access to a T-1 line. For example, the Naval European METOC Center (NEMOC) in Rota, Spain is hampered by an inadequate telecommunications infrastructure compared to Continental United States (CONUS) standards. This thesis addresses the operational feasibility of using the Global Broadcast Service (GBS), a global system of satellites providing a high speed broadcast service of video and data, for transferring large METOC data products from FNMOC to METOC regional centers around the world.

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Command, Control and Communications, Computing and Software

KEYWORDS: Global Broadcast Service, GBS, Satellite Communications, Bandwidth, Meteorology, Oceanography, Fleet Numerical Meteorological and Oceanography Center, FNMOC, Joint C^4I, C^4I, C^3, Joint Command, Control, Communications, Computers, and Intelligence Systems, Data Delivery

NETWORK DEFENSE-IN-DEPTH: EVALUATING HOST-BASED INTRUSION DETECTION SYSTEMS

Ronald E. Yun-Lieutenant, United States Navy
B.S., Strayer College, 1995
Master of Science in Systems Technology-June 2001
and
Steven A. Vozzola-Lieutenant, United States Navy
B.S., Jacksonville University, 1993
Master of Science in Systems Technology-June 2001
Advisor: Richard Harkins, Department of Physics
Second Reader: Daniel Warren, Department of Computer Science

As networks grow, their vulnerability to attack increases. DoD networks represent a rich target for a variety of attackers. The number and sophistication of attacks continue to increase as more vulnerabilities and the tools to exploit them become available over the Internet. The challenge for system administrators is to secure systems against penetration and exploitation while maintaining connectivity and monitoring and reporting intrusion attempts.

Traditional intrusion detection (ID) systems can take either a network or a host-based approach to preventing attacks. Many networks employ network-based ID systems. A more secure network will employ both techniques. This thesis will analyze the benefits of installing host-based ID systems, especially on the critical servers (mail, web, DNS) that lie outside the protection of the network ID system/Firewall. These servers require a layer of protection to ensure the security of the entire network and reduce the risk or attack..

Three host-based ID systems will be tested and evaluated to demonstrate their benefits on Windows 2000 Server. The proposed added security of host-based ID systems will establish defense-in-depth and work in conjunction with the network-based ID system to provide a complete security umbrella for the entire network.

DoD KEY TECHNOLOGY AREA: Computing and Software

KEYWORDS: Network Security, System Security, Intrusion Detection, Intrusion Detection System, Defense-in-depth